Attorney's Docket No.: 324-009927-US(PAR) *PATENT*

#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Express Mail No.: EL627420688US
In re application of: ALLAHWERDI et al. **Group No.:**
Serial No.: 0 /
Filed: Herewith **Examiner:**
For: METHOD AND ARRANGEMENT FOR RELIABLY IDENTIFYING A USER IN A COMPUTER SYSTEM

Commissioner of Patents and Trademarks
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country	**: Finland**
Application Number	**: 19992343**
Filing Date	**: 29 October 1999**

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added.)

SIGNATURE OF ATTORNEY

Reg. No.: 24,622

Clarence A. Green

Type or print name of attorney

Tel. No.: (203) 259-1800

Perman & Green, LLP

P.O. Address

Customer No.: 2512

425 Post Road, Fairfield, CT 06430

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 11.10.2000

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Mobile Phones Ltd** **Espoo**
Patenttihakemus nro Patent application no	**19992343**
Tekemispäivä Filing date	**29.10.1999**
Kansainvälinen luokka International class	**H04L**

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestely käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Menetelmä ja järjestely käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä

Keksinnön ala

Keksinnön kohteena on menetelmä ja järjestely käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä. Erityisesti keksintö kohdistuu ratkaisuun, jossa yhteys tietokonejärjestelmään toteutetaan matkaviestimen, edullisesti matkapuhelinjärjestelmän matkaviestimen avulla.

Keksinnön tausta

Useimmat tietokonejärjestelmät on suunniteltu siten, että käyttäjien täytyy kirjoittautua sisään järjestelmään työasemaltaan omalla käyttäjätunnuksellaan ja salasanallaan. Järjestelmän palvelin, tyypillisesti tunnistuspalvelin, tarkistaa onko kyseistä käyttäjätunnusta määritelty järjestelmän käyttäjien joukossa ja vastaako annettu salasana kyseistä käyttäjätunnusta. Mikäli näin on, sallitaan käyttäjän pääsy järjestelmään, muutoin yhteyttä ei sallita. Tällä tavoin pyritään varmistamaan järjestelmän turvallisuus eli estää asiattomien käyttäjien tunkeutuminen järjestelmään. Työasemien ollessa kiinteässä yhteydessä tietokonejärjestelmään esimerkiksi sisäisen kaapeloinnin välityksellä tämä menetelmä käyttäjien tunnistamiseksi on useimmiten riittävä.

Nykyisin on kuitenkin usein tarve tietokonejärjestelmän etäyhteyksiin. Tämä tarkoittaa sitä että käyttäjän työasemalla ei ole kiinteätä yhteyttä tietokonejärjestelmään, vaan yhteys muodostetaan jonkin julkisen verkon, tyypillisesti puhelinverkon välityksellä. Työasema kytketään esimerkiksi modeemin välityksellä puhelinverkkoon, jonka kautta muodostetaan puhelinyhteys järjestelmään järjestelmän modeemisarjan kautta. Tällaisessa tapauksessa käyttäjän tunnistukselle asetetaan huomattavasti suurempia vaatimuksia, koska yhteys muodostuu sellaisen julkisen verkon kautta, jonka turvallisuutta ei ole mahdollista valvoa järjestelmän ylläpitäjän toimesta. Käyttäjätunnukseen ja salasanaan perustuva käyttäjien tunnistus yleisen verkon yli tapahtuvassa yhteydessä on arveluttavaa, koska tällöin avautuu mahdollisuus ulkopuoliselle tunkeutua järjestelmään esimerkiksi arvaamalla käyttäjätunnuksia ja salasanoja. Käyttäjätunnukset sinänsä ovat usein käyttäjien nimistä muodostettuja ja mikäli käyttäjät saavat itse valita salasanansa, ovat ne sangen usein helposti pääteltävissä tai arvattavissa.

Päätelaitteen ja tietokonejärjestelmän väliset yhteydet on usein toteutettu ns. PPP (Point to point) protokollaa käyttäen. PPP-yhteyksillä on usein

käytetty ns. CHAP (Challenge-Handshake Authentication Protocol) tai PAP (Password Authentication Protocol) menetelmiä. PAP-menetelmässä salasana siirretään siirtotien ylitse kryptaamattomana, joten sen antama suoja on melko heikko. CHAP-menetelmä salasana on kryptattu. Menetelmässä siirtotien kummassakin päässä käytetään samaa algoritmia. Verkko lähettää satunnaisluvun päätteelle, pääte laskee luvun, käyttäjätunnuksen ja salasanan perusteella algoritmia käyttäen salatun arvon. Salattu arvo, salasana ja käyttäjätunnus välitetään verkolle, joka laskee salatusta arvosta salasanan, ja vertaa sitä lähetettyyn salasanaan.

Edelleen on tunnettua käyttää ns. RADIUS (Remote Authentication Dial In User Service Protocol, RFC 2138) menetelmää sisäänkirjautumisen yhteydessä.

On edelleen kehitetty erilaisia menetelmiä tietokonejärjestelmän käyttäjän tunnistuksen luotettavuuden ja turvallisuuden lisäämiseksi. Koska käyttäjän määrittelemät ovat usein helposti selvitettävissä, on tunnetun tekniikan mukaisissa ratkaisuissa hyödynnetty kertakäyttöisiä salasanoja. Tällöin kutakin salasanaa käytetään vain kerran sisäänkirjoittautumisen yhteydessä ja vaikka salasanan saisi jokin kolmas osapuoli selville, ei siitä olisi mitään hyötyä koska toisella kerralla käytössä olisi jo jokin muu salasana. Tässä menetelmässä täytyy sekä käyttäjällä että tietokonejärjestelmän tunnistuspalvelimella olla toisiansa vastaavat salasanalistat käytössä. Käyttäjällä voi olla esimerkiksi salasanalista paperilla tai vaihtoehtoisesti voidaan käyttää erillistä laitetta, ns. trusted device, jota käytetään generoimaan kertakäyttöisiä salasanoja.

Patenttijulkaisussa US 5485519 on esitetty menetelmä, jossa käyttäjällä on erillinen salasanan tuottava laite. Käyttäjä syöttää laitteeseen jonkin ennalta sovitun salasanan, ja laite muodostaa salasanasta ja laitteeseen ohjelmoidusta kryptatusta bittijonosta yhteydellä käytettävän salasanan. Tämä salasana kryptataan, tallennetaan laitteeseen ja sitä käytetään seuraavan salasanan generointiin. Julkaisun ratkaisussa laitteen kehittämä salasana on syötettävä esim. magneettiraitalukijan tai levykeaseman välityksellä yhteyden muodostavaan prosessorilaitteistoon, kuten esimerkiksi tietokoneeseen.

Patenttijulkaisussa US 4720860 esitetään kertakäyttöisiä salasanoja käyttävä ratkaisu, jossa käyttäjällä on erillinen laite, esimerkiksi smart card- tyyppinen kortti, joka generoi kertakäyttöisen salasanan, jonka käyttäjä lukee laitteen näytöstä ja syöttää yhteysvälineenä toimivaan tietokoneeseen.

Laite generoi kertakäyttöisen koodin kiinteän koodin ja jonkin muuttuvan parametrin kuten ajan perusteella. Kiinteä koodi on ohjelmoitu laitteeseen. On myös mahdollista, että kiinteä koodi syötetään laitteeseen. Tietokonejärjestelmän tunnistuspalvelin laskee samoja parametrejä käyttäen toisen tunnusluvun, ja jos tunnusluvut täsmäävät, niin yhteys on sallittu ja mahdollinen.

Patenttijulkaisuissa US 5657388, US 5373559 ja 5491752 esitetään toinen kertakäyttöisiä salasanoja käyttävä ratkaisu, jossa käyttäjällä on erillinen yksinkertainen laite, ns. token, joka on esimerkiksi muistikortti, ja johon on tallennettu salainen koodi. Yhteysväline, esimerkiksi kannettava tietokone, lukee kortin muistista salaisen koodin. Käyttäjä syöttää yhteysvälineelle henkilökohtaisen salasanansa, ja yhteysväline muodostaa salaisen koodin, salasanan ja ajan perusteella kertakäyttöisen salasanan, jonka se lähettää tietokonejärjestelmän tunnistuspalvelimelle.

Kaikissa yllä kuvatuissa tunnetun tekniikan mukaisissa ratkaisuissa käyttäjän on pidettävä mukanaan useampia laitteita, eli sekä erillistä salasanan muodostuksessa käytettävää generointilaitetta, tyypillisesti smart card -tyyppistä älykorttia, sekä varsinaista yhteyslaitetta, jolla yhteys haluttuun tietokonejärjestelmään muodostetaan. Edelleen kaikissa tunnetuissa ratkaisuissa käyttäjän on aktiivisesti joko kirjoitettava älykortista luettu kertakäyttöinen salasana yhteysvälineeseen tai vaihtoehtoisesti syötettävä koko kortti yhteysvälineeseen, jolloin kortin tiedot tulevat luetuiksi.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten toteuttaa menetelmä ja menetelmän toteuttava järjestely siten, että käyttäjä voidaan luotettavasti tunnistaa aiheuttamatta kuitenkaan haittaa tai vaivaa käyttäjälle. Tämä saavutetaan menetelmällä käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä, jossa menetelmässä käytetään yhteyslaitteena tietokonejärjestelmään matkaviestintä, syötetään henkilökohtainen tunnusluku matkaviestimeen.

Keksinnön mukaisessa menetelmässä generoidaan ensimmäinen kertakäyttöinen salasana matkaviestimessä ilman käyttäjän toimenpiteitä ennalta tunnetun algoritmin avulla käyttäjän henkilökohtaisen tunnusluvun, matkaviestimen tilaajakohtaiselta tunnistusmoduulilta luetun tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, suoritetaan ensimmäisen kertakäyttöisen salasanan ja käyttäjän tilaajakohtaisen tunnisteen koodaus matkaviestimessä, lähetetään koodatut salasana ja tilaajakohtainen tunniste tietokonejärjestelmän tunnistuspalvelimelle, suorite-

taan käyttäjän tunnistus tunnistuspalvelimella tilaajakohtaisen tunnisteen perusteella ja etsitään tietokannasta käyttäjän henkilökohtainen tunnusluku ja käyttäjään liitetyn matkaviestimen laitekohtainen tunniste, muodostetaan toinen kertakäyttöinen salasana tunnistuspalvelimella käyttäen ennalta määrättyä algoritmia käyttäjän henkilökohtaisen tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, verrataan ensimmäistä salasanaa ja toista salasanaa keskenään tunnistuspalvelimella, ja mikäli salasanat vastaavat, mahdollistetaan tietoliikenneyhteys käyttäjän matkaviestimen ja tietokonejärjestelmän välillä.

Keksinnön kohteena on myös järjestely käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä, joka järjestely käsittää matkaviestimen, jota käytetään yhteyslaitteena tietokonejärjestelmään, joka matkaviestin käsittää tilaajakohtaisen tunnistusmoduulin, joka sisältää tilaajakohtaisen tunnisteen, viestimeen pysyvästi koodatun laitekohtaisen tunnisteen, välineet lukea käyttäjän syöttämä henkilökohtainen tunnusluku, joka mahdollistaa laitteen käytön, välineet tarkistaa tunnusluvun oikeellisuus ennen laitteen kutakin käyttöönottoa, ja joka järjestely käsittää tunnistuspalvelimen, joka käsittää muistivälineet tallentaa järjestelmän käyttäjien käyttäjätunnukset ja niitä vastaavat henkilökohtaiset tunnisteet ja laitekohtaiset tunnisteet.

Keksinnön mukaisessa järjestelyssä matkaviestin käsittää välineet generoida ensimmäinen kertakäyttöinen salasana ilman käyttäjän toimenpiteitä ennalta tunnetun algoritmin avulla käyttäjän henkilökohtaisen tunnusluvun, matkaviestimen tilaajakohtaiselta tunnistusmoduulilta luetun tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, välineet suorittaa ensimmäisen kertakäyttöisen salasanan ja käyttäjän tilaajakohtaisen tunnisteen koodaus, välineet lähettää koodatut salasana ja tilaajakohtainen tunniste tietokonejärjestelmän tunnistuspalvelimelle, ja että tunnistuspalvelin on sovitettu suorittamaan käyttäjän tunnistus tilaajakohtaisen tunnisteen perusteella ja etsimään tietokannasta käyttäjän henkilökohtainen tunnusluku ja käyttäjään liitetyn matkaviestimen laitekohtainen tunniste, muodostamaan toinen kertakäyttöinen salasana tunnistuspalvelimella käyttäen ennalta määrättyä algoritmia käyttäjän henkilökohtaisen tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, vertaamaan ensimmäistä salasanaa ja toista salasanaa keskenään tunnistuspalvelimella, ja mikäli salasanat vastaavat, mahdollistamaan tietoliikenneyhteys käyttäjän matkaviestimen ja tietokonejärjestelmän välillä.

Keksintö perustuu siihen, että matkaviestin itse on ns. trusted device, jolloin käyttäjältä ei vaadita erillisiä laitteita mukana pidettäväksi, kun halutaan muodostaa turvallinen yhteys tietokonejärjestelmään. Keksinnön mukaisella ratkaisulla voidaan myös yhteydenmuodostus automatisoida turvallisuuden siitä kärsimättä.

Keksinnön mukaisessa ratkaisussa siis matkaviestin, jolla muodostetaan yhteys tietokonejärjestelmään, generoi itse tarvittavan kertakäyttöisen salasanan. Salasanan generoinnissa käytetään ennalta määrättyä algoritmia, jonka parametreinä ovat aika, käyttäjän tilaajatunnus, matkaviestimen laitetunnus ja käyttäjän PIN-koodi.

Keksinnön mukaisen menetelmällä ja järjestelmällä saavutetaan useita etuja. Aiempien ratkaisujen eräs haittapuoli, eli kahden erillisen laitteen käyttö, voidaan välttää. Itse yhteydenmuodostusprosessi on myös aiempaa nopeampi, koska käyttäjän ei tarvitse tässä vaiheessa syöttää laitteeseen salasanoja tai ulkopuolisia lisälaitteita. Keksinnön mukainen ratkaisu on myös tietoturvallinen, sillä kertakäyttöisten salasanojen, käytettyjen algoritmien tai ohjelmien sieppaus eivät auta mahdollista tunkeutujaa. Kopioidut ohjelmistot eivät toimi vieraassa laitteessa vaikka käyttäjän salasana (PIN) olisi saatu selville.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joissa

kuvio 1 esittää esimerkkiä järjestelmästä, jossa keksinnön mukaista ratkaisua voidaan soveltaa,

kuviot 2a ja 2b havainnollistavat keksinnön mukaista menetelmää vuokaavioiden avulla, ja

kuvio 3 havainnollistaa esimerkkiä keksinnön mukaisen matkaviestimen rakenteesta.

Keksinnön yksityiskohtainen selostus

Viitaten kuvioon 1 tarkastellaan esimerkkiä eräästä järjestelmästä, jossa keksinnön mukaista ratkaisua voidaan soveltaa. Keksinnön mukaisessa ratkaisussa käyttäjällä on matkaviestin 100, jota hän käyttää yhteysvälineenä haluamaansa tietokonejärjestelmään 102. Kuviossa 1 on esitetty vain eräs esimerkki keksinnön mukaisesta radiojärjestelmästä. Sinänsä radiojärjestelmään rakenne ja yhteys tietokonejärjestelmään voi olla yksityiskohdiltaan to-

teutettu muutoinkin, kunhan keksinnön mukaiset piirteet ovat mukana. Keksinnön mukainen ratkaisu ei siis rajoitu pelkästään GPRS-järjestelmään, vaikka sellaista onkin käytetty esimerkkinä kuviossa 1.

Radioverkko käsittää siis tyypillisesti kiinteän verkon infrastruktuurin eli verkko-osan 104, ja tilaajapäätelaitteita 100, jotka voivat olla kiinteästi sijoitettuja, ajoneuvoon sijoitettuja tai kannettavia mukanapidettäviä päätelaitteita. Verkko-osassa 104 on tukiasemia 106. Useita tukiasemia 106 keskitetysti puolestaan ohjaa niihin yhteydessä oleva radioverkkokontrolleri 108. Tukiasemassa 106 on lähetinvastaanottimia 110 ja multiplekseriyksikkö 112.

Tukiasemassa 106 on edelleen ohjausyksikkö 114, joka ohjaa lähetinvastaanottimien 110 ja multiplekserin 112 toimintaa. Multiplekserillä 112 sijoitetaan useiden lähetinvastaanottimen 110 käyttämät liikenne- ja ohjauskanavat yhdelle siirtoyhteydelle 116.

Tukiaseman 106 lähetinvastaanottimista 110 on yhteys antenniyksikköön 118, jolla toteutetaan kaksisuuntainen radioyhteys 120 tilaajapäätelaitteeseen 100. Kaksisuuntaisessa radioyhteydessä 120 siirrettävien kehysten rakenne on järjestelmäkohtaisesti määritelty, ja sitä kutsutaan ilmarajapinnaksi.

Radioverkkokontrolleri 108 käsittää ryhmäkytkentäkentän 122 ja ohjausyksikön 124. Ryhmäkytkentäkenttää 124 käytetään puheen ja datan kytkentään sekä yhdistämään signalointipiirejä. Tukiaseman 106 ja radioverkkokontrollerin 108 muodostamaan radioverkkoalijärjestelmään 126 kuuluu lisäksi transkooderi 128. Transkooderi 128 sijaitsee yleensä mahdollisimman lähellä matkapuhelinkeskusta 130, koska puhe voidaan tällöin siirtokapasiteettia säästäen siirtää solukkoradioverkon muodossa transkooderin 128 ja radioverkkokontrollerin 108 välillä.

Transkooderi 128 muuntaa yleisen puhelinverkon ja radiopuhelinverkon välillä käytettävät erilaiset puheen digitaaliset koodausmuodot toisilleen sopiviksi, esimerkiksi kiinteän verkon muodosta solukkoradioverkon johonkin muuhun muotoon ja päinvastoin. Ohjausyksikkö 124 suorittaa puhelunohjausta, liikkuvuuden hallintaa, tilastotietojen keräystä ja signalointia.

Kuviossa 1 kuvataan edelleen matkapuhelinkeskus 130 ja porttimatkapuhelinkeskus 132, joka hoitaa matkapuhelinjärjestelmän yhteydet ulkopuoliseen maailmaan, tässä yleiseen puhelinverkkoon 134. Matkapuhelinjärjestelmä käsittää myös erilaisia tietokantoja, joissa ylläpidetään erilaisia tietoja järjestelmän toimivuuden ylläpitämiseksi. Tällainen rekisteri on HLR 150 (Home Location Register), joka sisältää järjestelmän tilaajiin liittyvää informaa-

tiota. HLR pitää esimerkiksi tietoa siitä, missä tilaaja kulloinkin sijaitsee. Edelleen järjestelmässä on loogisesti MSC-kohtainen VLR 152 (Visitors Location Register), joka ylläpitää tietoa siitä, kuka käyttäjä on kulloinkin annetun MSC:n alueella ja tietoa käyttäjän sijainnista tarkemmin kuin HLR. Edelleen järjestelmässä on EIR 154 (Equipment Identity Register), joka ylläpitää tieto järjestelmän päätelaitteista. Kullakin päätelaitteella on tyypillisesti laitekohtainen valmistusvaiheessa liitetty laitetunnus, esim. IMEI-tunnus (International Mobile Equipment Identifier), jonka perusteella kukin päätelaite voidaan yksilöllisesti tunnistaa. EIR ylläpitää tietoa laitetunnuksista.

Kuten kuviosta 1 nähdään niin ryhmäkytkentäkentällä 122 voidaan suorittaa kytkentöjä sekä yleiseen puhelinverkkoon (PSTN = Public Switched Telephone Network) 134 matkapuhelinkeskuksen 130 välityksellä että pakettisiirtoverkkoon 136.

Pakettisiirtoverkon 136 ja ryhmäkytkentäkentän 122 välisen yhteyden luo tukisolmu 138 (SGSN = Serving GPRS Support Node). Tukisolmun 138 tehtävänä on siirtää paketteja tukiasemajärjestelmän ja porttisolmun (GGSN = Gateway GPRS Support Node) 140 välillä, ja pitää kirjaa tilaajapäätelaitteen 100 sijainnista alueellaan. Tukisolmu 138 voi olla yhteydessä myös matkapuhelinjärjestelmän tietokantoihin 150 - 154 joko MSC:n 130 kautta tai suoraan.

Porttisolmu 140 yhdistää julkisen pakettisiirtoverkon 142 ja pakettisiirtoverkon 132. Rajapinnassa voidaan käyttää internet-protokollaa tai X.25-protokollaa. Porttisolmu 140 kätkee kapseloimalla pakettisiirtoverkon 136 sisäisen rakenteen julkiselta pakettisiirtoverkolta 142, joten pakettisiirtoverkko 136 näyttää julkisen pakettisiirtoverkon 142 kannalta aliverkolta, jossa olevalle tilaajapäätelaitteelle 100 julkinen pakettisiirtoverkko voi osoittaa paketteja ja jolta voi vastaanottaa paketteja.

Pakettisiirtoverkko 136 on tyypillisesti radioverkko-operaattorin internet-protokollaa käyttävä verkko, joka kuljettaa signalointia ja tunneloitua käyttäjän dataa. Verkon 136 rakenne voi vaihdella operaattorikohtaisesti sekä arkkitehtuuriltaan että protokolliltaan internet-protokollakerroksen alapuolella.

Julkinen pakettisiirtoverkko 142 voi olla esimerkiksi maailmanlaajuinen Internet, johon tietokonejärjestelmä 102 on yhdistetty.

Tietokonejärjestelmä 102 käsittää tyypillisesti jonkin tunnistuspalvelimen 144, jonka tehtävänä on autentisoida järjestelmään pyrkivät käyttäjät ja sallia luvallisten käyttäjien pääsyn muuhun järjestelmään 146. Tunnistuspalvelin 144 ei välttämättä ole erillinen laitteisto, vaan se voidaan toteuttaa myös ohjelmallisesti jonkin tietokoneen osana. Tunnistuspalvelin käsittää myös

muistin 148, jojon on tallennettu järjestelmän käyttäjien käyttäjätunnukset ja niitä vastaavat henkilökohtaiset tunnisteet ja laitekohtaiset tunnisteet. Muisti voidaan toteuttaa kiinteänä osana normaalia palvelinlaitteistoa tai erillisenä tietokantalaitteistona. Muu järjestelmä 146 käsittää tyypillisesti yhden tai useampia tietokonelaitteistoja, jotka tarjoavat sähköposti- tai tietokantapalveluja ja vastaavia yrityksen sisäistä verkkoratkaisuja.

Tukisolmusta 138 voidaan muodostaa toisen porttisolmun 140b kautta yhteys toiseen dataverkkoon 156, edullisesti paikallisverkkoon kuten esimerkiksi yrityksen sisäinen intranet. Keksinnön mukaisessa ratkaisussa voidaan siis yhteys haluttuun tunnistautumista vaativaan verkkoon muodostaa useilla tavoilla.

Esillä oleva keksintö liittyy siis erityisesti käyttäjän luotettavaan tunnistamiseen otettaessa yhteyttä tietokonejärjestelmään. Vaikka tunnistuksen on oltava luotettava, on myös toivottavaa, että tunnistusproseduuri voidaan toteuttaa käyttäjän kannalta vaivattomasti.

Tarkastellaan esimerkkiä keksinnön mukaisesta ratkaisusta vuokaavioiden 2a ja 2b avulla. Vaiheessa 200 käyttäjä käynnistää matkaviestimen. Tyypillisesti matkaviestin on sovitettu tässä vaiheessa kysymään käyttäjältä matkaviestimen käytön mahdollistavan salasanan eli PIN:n (Personal Identification Number). Vaiheessa 202 käyttäjä syöttää salasanan matkaviestimeen. Matkaviestintä voi tällöin käyttää myös tavanomaisena puhelimena, mutta kun käyttäjä vaiheessa 204 käynnistää jonkin ennalta määrättyä tietokonejärjestelmää tarvitsevan sovelluksen, kuten esimerkiksi sähköpostiohjelman, keksinnön mukaisessa ratkaisussa matkaviestin tällöin generoi kertakäyttöisen salasanan vaiheessa 206. Tätä vaihetta selostetaan tarkemmin tuonnempana.

Mikäli matkaviestintä ei ole tarkoitus käyttää salausta vaativaan viestintään, käyttäjä voi viestimen käynnistyksen yhteydessä syöttää viestimeen jonkin muun ennalta määrätyn salasanan eli PIN:n. Käyttäjällä on siis keksinnön edullisessa toteutusmuodossa hallussaan ainakin kaksi eri salasanaa, joista osa mahdollistaa salausta vaativien sovellusten käytön ja osa ei. Täten matkaviestintä voidaan turvallisesti käyttää ja haluttaessa myös lainata toiselle osapuolelle, joka ei pysty salausta vaativia sovelluksia käyttämään.

Seuraavaksi matkaviestin tyypillisesti koodaa generoidun salasanan ja käyttäjän käyttäjätunnuksen sopivalla tavalla ja lähettää viestin tietokonejärjestelmälle vaiheessa 208. Tietokonejärjestelmä vastaanottaa viestin, ja

vaiheessa 210 generoi itse vastaavan kertakäyttöisen salasanan, vertaa salasanoja, ja mikäli salasanat täsmäävät myöntää oikeuden järjestelmän tietoihin, ja yhteys voi jatkua vaiheessa 212. Mikäli salasanat eivät täsmää, järjestelmä ei keksinnön edullisessa toteutusmuodossa lähetä mitään vastinetta matkaviestimelle. Tämä lisää turvallisuutta, koska mahdollinen tunkeutuja ei saa selville yhteyden epäonnistumisen syytä.

Salasana ja käyttäjätunnuksen lähetys tietokonejärjestelmälle voidaan suorittaa sopivalla tavalla kryptattuna, joko käyttäen radiojärjestelmälle ominaista kryptausta tai turvallisuutta lisäävällä omalla kryptauksella, jonka vastaanottopää osaa purkaa. Nämä vaiheet voidaan toteuttaa alan ammattimiehelle tunnetuilla tavoilla.

Salasanan generointia havainnollistetaan tarkemmin kaaviossa 2b. Vaiheessa 220 matkaviestin tahdistaa sisäisen kellonsa samaan tahtiin järjestelmän kellon kanssa. Tämä tahdistus voi tapahtua tunnettuja tahdistusmenetelmiä käyttäen. Tahdistumisen tarkoituksen on varmentaa, että matkaviestimessä ja järjestelmässä käytetään samaa aikaparametria salasanoja generoitaessa. Vaiheessa 222 luetaan käyttäjän ns. A-tilaajatunnus (A_SCRBR) matkaviestimen tilaajakohtaiselta tunnistusmoduulilta, kuten SIM/USIM-kortilta ([Universal] Subscriber Identity Module) tai vastaavalta.

Vaiheessa 224 luetaan matkaviestimen laitetunnus. Keksinnön mukaisessa ratkaisussa kullakin matkaviestimellä on laitekohtainen matkaviestimeen valmistusvaiheessa liitetty laitetunnus, esim. IMEI-tunnus (International Mobile Equipment Identifier), jonka perusteella kukin matkaviestin voidaan yksilöllisesti tunnistaa. Esimerkiksi GSM-järjestelmässä IMEI-tunnus käsittää seuraavat kentät:

TAC type approval code,
FAC final assembly code,
SNR serial number,
SVN software version number.

Vaiheessa 226 luetaan käyttäjän syöttämä henkilökohtainen tunnusluku, PIN, muistista.

Käyttäen yllämainittuja arvoja (käyttäjän henkilökohtainen tunnusluku (PIN), tilaajakohtainen tunniste (A_SCRBR), matkaviestimen laitekohtainen tunnisteen (IMEI) ja kellonaika), matkaviestin laskee ennalta määrättyä algoritmia käyttäen kertakäyttöisen salasanan. Ennalta määrätty algoritmi voi olla

kiinteästi ohjelmoitu matkaviestimeen, tai vaihtoehtoisesti se voi olla muutettavissa, esimerkiksi ladattavissa tietokonejärjestelmästä.

Edellä mainittujen arvojen lisäksi on myös mahdollista käyttää eräänä algoritmiparametrina matkaviestimen muistiin tallennettuja lukuja. Tietokonejärjestelmästä voidaan esimerkiksi ladata taulukkomuodossa joukko alkulukuja. Sama taulukko on myös tunnistuspalvelimen tiedossa.

Vaihtamalla matkaviestimen PIN voidaan viestin antaa myös ulkopuolisen käyttöön, koska tällöin ei yhteyttä tietokonejärjestelmään ole mahdollista muodostaa. Tällöin pääte voi joko estää tunnistusproseduurin käynnistymisen kokonaan tai sallia tunnistusproseduurin; tällöinhän yhteyden luonti aina epäonnistuu, koska PIN on väärä. Samoin SIM-korttia vaihtamalla voidaan yhteyden muodostus estää.

Keksinnön mukaiset erityispiirteet voidaan edullisesti toteuttaa sekä matkaviestimessä että tietokonejärjestelmässä ohjelmallisesti. Tarkastellaan seuraavaksi esimerkkiä matkaviestimen rakenteesta kuvion 3 avulla.

Kuviossa 3 kuvataan esimerkkiä yhden matkaviestimen 100 rakenteesta. Matkaviestin käsittää antennin 300, jota käytetään signaalien lähetykseen ja vastaanottoon. Tarkastellaan ensin vastaanotinpuolta. Antennilla 300 vastaanotettu signaali viedään duplexsuodattimen 302 kautta radiotaajuusvastaanottimelle 304. Duplexsuodatin erottaa lähetys- ja vastaanotintaajuudet toisistaan. Radiotaajuusvastaanotin 304 käsittää suodattimen, joka estää halutun taajuuskaistan ulkopuoliset taajuudet. Sen jälkeen signaali muunnetaan välitaajuudelle tai suoraan kantataajuudelle, jossa muodossa oleva signaali näytteistetään ja kvantisoidaan analogia/digitaalimuuntimessa 306. Ekvalisaattori 308 kompensoi häiriöitä, esimerkiksi monitie-etenemisen aiheuttamia häiriöitä. Demodulaattori 310 ottaa ekvalisoidusta signaalista bittivirran, joka välitetään demultiplekserille 312. Demultiplekseri 312 erottelee bittivirran eri aikaväleistä omiin loogisiin kanaviinsa. Kanavakoodekki 314 dekoodaa eri loogisten kanavien bittivirran, eli päättää onko bittivirta signalointitietoa, joka välitetään ohjausyksikölle 316, vai onko bittivirta puhetta, joka välitetään puhekoodekille 318, tai dataa, joka välitetään esimerkiksi datayksikölle 320. Datayksikkö voi olla esimerkiksi viestimen näyttö tai jokin dataa prosessoiva yksikkö, lisälaite tai vastaava. Puhekoodekilta 318 puhesignaali välitetään edelleen kaiuttimelle 322. Kanavakoodekki 314 suorittaa myös virheenkorjausta. Ohjausyksikkö 316 suorittaa sisäisiä kontrollitehtäviä ohjaamalla eri yksikköjä.

Lähetyspuolella kanavakoodekille 314 tulee lähetettävä signaali joko datayksiköltä 320 tai puhekoodekilta 318. Puhekoodekille signaali tulee mik-

rofonilta 324. Datayksikkö voi olla esimerkiksi näppäimistö tai kosketusherkkä näyttö tai jokin viestimen lisälaite. Purskemuodostin 326 lisää opetussekvenssin ja hännän kanavakoodekista 314 tulevaan dataan. Multiplekseri 328 osoittaa kullekin purskeelle sen aikavälin. Modulaattori 330 moduloi digitaaliset signaalit radiotaajuiselle kantoaallolle. Tämä toiminto on analoginen luonteeltaan, joten sen suorittamisessa tarvitaan digitaali/analogia-muunninta 332. Lähetin 334 käsittää suodattimen, jolla kaistanleveyttä rajoitetaan. Lisäksi lähetin 334 kontrolloi lähetyksen ulostulotehoa. Syntetisaattori 336 järjestää tarvittavat taajuudet eri yksiköille. Syntetisaattori 336 luo tarvitut taajuudet esimerkiksi jänniteohjatulla oskillaattorilla.

Kuviossa 3 esitettävällä tavalla voidaan lähetinvastaanottimen rakenne jakaa vielä radiotaajuusosiin 338 ja digitaaliseen signaalinkäsittelyprosessoriin ohjelmistoineen 340. Radiotaajuusosiin 338 kuuluvat duplexsuodatin 302, vastaanotin 304, lähetin 334 ja syntetisaattori 336. Digitaaliseen signaalinkäsittelyprosessoriin ohjelmistoineen 340 kuuluvat ekvalisaattori 308, demodulaattori 310, demultiplekseri 312, kanavakoodekki 314, ohjausyksikkö 316, purskemuodostin 326, multiplekseri 328 ja modulaattori 330. Analogisen radiosignaalin muuntamiseksi digitaaliseksi signaaliksi tarvitaan analogia/digitaalimuunnin 306, ja vastaavasti digitaalisen signaalin muuntamiseksi analogiseksi signaaliksi digitaali/analogia-muunnin 332.

Matkaviestin käsittää edelleen tilaajakohtaisen tunnistusmoduulin lukulaitteen 342, tyypillisesti SIM/USIM-kortin lukulaitteen tai vastaavan. Kun matkaviestin käynnistetään, viestimen ohjausyksikkö 316 tarkistaa onko lukulaitteessa korttia, ja lukee kortilta käyttäjän tunnistustiedot. Matkaviestimeen on edelleen tallennettu viestimen valmistusvaiheessa muistielementtiin 344 viestimen laitekohtainen tunniste (IMEI), joka on ohjausyksikön 316 luettavissa. Laitekohtaista tunnistetta säilytetään kiinteästi muistipiirissä eikä se ole helposti muuteltavissa.

Keksinnön mukainen laite voi käsittää luonnollisesti erilaisia käyttöliittymäosia, kuten näytön ja näppäimistön, mutta niitä ei tässä ole tarkemmin kuvattu.

Keksinnön mukaiset toiminnot voidaan toteuttaa matkaviestimessä siis edullisesti ohjelmallisesti. Tarvittavat toimintokäskyt käsittävä ohjelmisto voidaan sijoittaa ohjausyksikön 316 yhteyteen. Ohjelmisto voi rakenteeltaan luonnollisesti olla modulaarinen, eli koostua useasta erillisestä ohjelmasta, joita voidaan erikseen päivittää esimerkiksi tietokonejärjestelmästä tai radioverkon operaattorilta käsin.

Keksinnön mukaista ratkaisua voidaan soveltaa myös sellaisessa matkaviestimessä, jotka on varustettu useammalla kuin yhdellä SIM/USIM-kortilla. Tällaisia ovat esimerkiksi puhelimet, joissa voidaan käyttää ns. ennakkoon maksettuja SIM/USIM-kortteja (pre-paid SIM/USIM). Tällaisessa viestimessä on mahdollista ratkaisu, että vain yhtä korttia käytetään yhteyden muodostamiseen. Keksinnön eräässä toteutusmuodossa osa salaukseen tarvittavista tiedoista saadaan siitä kortista, jota ei yhteyden muodostuksessa käytetä.

Tarkastellaan seuraavaksi erästä toista keksinnön edullista toteutusmuotoa. Esimerkiksi GSM ja GPRS-järjestelmissä yhteydenmuodostusta suoritettaessa sekä päätelaitteella että verkolla on tiedossa ns SRES kenttä (Signed RESult). Kentästä on myös käytetty lyhennettä XRES. Kenttä on tyypillisesti 32 - 128 bitin mittainen kenttä. Yhteydenmuodostuksen yhteydessä SRES määritetään yhteyden kummankin osapuolen toimesta tietyillä yhteisillä parametrejä käyttäen samaa algoritmia. Tunnetun tekniikan mukaisessa ratkaisussa SRES siirretään päätelaitteesta verkkoon, jossa laskettua lukua verrataan verkossa laskettuun lukuun. SRES-kentästä löytyy lisätietoja esimerkiksi kirjasta M. Mouly, M_P. Pautet: The GSM System for Mobile Communications. ISBN 2-9507190-0-7, luku 7.2.2.1., joka otetaan tähän viitteeksi.

Keksinnön tässä toteutusmuodossa päätelaite lähettää pelkän SRES:n sijasta tiedon, joka voi käsittää kentät

SRES	Signed result
TIME	aikatieto
IMSI	päätteen kansainvälinen numero
IMEI	päätteen laitenumero.

Tämän toteutusmuodon etuna verrattuna tunnettuun tekniikkaan on luonnollisesti parantunut suojaus, sillä se on sekä aika- että laitekohtainen. Päätteen kansainvälinen numero IMSI koostuu GSM-pohjaisissa järjestelmissä päätteen maakoodista, operaattorin koodista sekä varsinaisesta päätteen puhelinnumerosta.

Tarkastellaan seuraavaksi edelleen erästä toista keksinnön edullista toteutusmuotoa. Käytettäessä RADIUS protokollaa PPP/CHAP-menetelmän yhteydessä tunnistuspalvelin vastaanottaa päätelaitteelta kentät "chap challenge", "user name", "chap response". Tunnistuspalvelin vertaa itse generoimaansa "chap responsea" päätelaitteelta vastaanottamaansa. Keksinnön tämän toteutusmuodon mukaisessa ratkaisussa kentillä on arvot:

"chap challenge" SRES

"user name" käyttäjätunnus järjestelmään

"chap response" sana joka on muodostettu arvoista (IMSI, IMEI, PIN, aika, SRES).

Koska kentissä on mukana käyttäjätunnus järjestelmään selväkielisenä, niin tunnistuspalvelin pystyy siis nopeasti valitsemaan omasta tietokannastaan muut tiedot ja generoimaan ajasta riippuvaisen paikallisen "chap responsen", jonka on siis vastattava päätelaitteelta vastaanotetun kanssa.

Edelleen keksinnön eräässä toisessa edullisessa toteutusmuodossa käytetään muunnettua PPP/PAP- menetelmää RADIUS protokollan yhteydessä. PPP/PAP -menetelmässähän alun perin lähetettiin käyttäjätunnus ja salasana kryptaamattomana siirtotien yli, jolloin suojaus on heikko. Keksinnön mukaisessa ratkaisussa käyttäjätunnukselle varatussa kentässä lähetetäänkin keksinnön mukaisesti muodostettu salattu tunnus, joka perustuu arvoille (IMSI, IMEI, PIN, aika, SRES). Salasanalle varatussa kentässä lähetetään SRES. Edelleen käyttäjätunnus järjestelmään lähetetään "Calling station id"-kentässä. Tämä sen takia, että tunnistuspalvelin voi tunnistaa soittajan käymättä kaikkia mahdollisia käyttäjiä lävitse. RADIUS-menetelmää käytettäessä salasanalle varattu kenttä (jossa nyt lähetetäänkin SRES) voidaan suojata GGSN:n ja yritysverkon yhteisellä avaimella. Keksinnön tämän toteutusmuodon mukaisessa ratkaisussa kentillä on siis arvot:

"user name" sana joka on muodostettu arvoista (IMSI, IMEI, PIN, aika, SRES),

"user password" SRES,

"Calling station id" käyttäjätunnus järjestelmään.

Keksinnön eräässä edullisessa toteutusmuodossa edellä kuvatuissa vaihtoehdoissa käyttäjätunnus järjestelmään on sama kuin käyttäjän ISDN-muodossa oleva puhelinnumero, eli ns. MSISDN. Tästä löytyy lisätietoja esimerkiksi kirjasta M. Mouly, M_P. Pautet: The GSM System for Mobile Communications. ISBN 2-9507190-0-7, luku 8.1.1., joka otetaan tähän viitteeksi.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaiseen esimerkkiin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella monin tavoin oheisten patenttivaatimusten esittämän keksinnöllisen ajatuksen puitteissa.

Patenttivaatimukset

1. Menetelmä käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä (102), jossa menetelmässä käytetään yhteyslaitteena tietokonejärjestelmään matkaviestintä (100), syötetään henkilökohtainen tunnusluku matkaviestimeen,

t u n n e t t u siitä, että

generoidaan ensimmäinen kertakäyttöinen salasana matkaviestimessä ilman käyttäjän toimenpiteitä ennalta tunnetun algoritmin avulla käyttäjän henkilökohtaisen tunnusluvun, matkaviestimen tilaajakohtaiselta tunnistusmoduulilta (342) luetun tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen (IMEI) ja kellonajan perusteella, suoritetaan ensimmäisen kertakäyttöisen salasanan ja käyttäjän tilaajakohtaisen tunnisteen koodaus matkaviestimessä, lähetetään koodatut salasana ja tilaajakohtainen tunniste tietokonejärjestelmän (102) tunnistuspalvelimelle (144), suoritetaan käyttäjän tunnistus tunnistuspalvelimella tilaajakohtaisen tunnisteen perusteella ja etsitään tietokannasta käyttäjän henkilökohtainen tunnusluku ja käyttäjään liitetyn matkaviestimen laitekohtainen tunniste, muodostetaan toinen kertakäyttöinen salasana tunnistuspalvelimella käyttäen ennalta määrättyä algoritmia käyttäjän henkilökohtaisen tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, verrataan ensimmäistä salasanaa ja toista salasanaa keskenään tunnistuspalvelimella, ja mikäli salasanat vastaavat, mahdollistetaan tietoliikenneyhteys käyttäjän matkaviestimen (100) ja tietokonejärjestelmän (102) välillä.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että matkaviestin (100) tahdistaa matkaviestimen ajastuksen tunnistuspalvelimen (144) ajastuksen kanssa ennen tunnistusproseduurin käynnistystä.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että käyttäjän tunnistus suoritetaan automaattisesti käyttäjän käynnistäessä tietokonejärjestelmää (102) hyödyntävän sovelluksen matkaviestimessä (100).

4. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että mikäli ensimmäinen ja toinen salasana eivät vastaa, tunnistuspalvelin (144) ei lähetä mitään informaatiota matkaviestimelle (100).

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tunnistuksen aikana päätelaite lähettää tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka si-

sältönä on aika, sekä kentän, jonka sisältönä on päätteen kansainvälinen puhelinnumero, sekä kentän, jonka sisältönä on päätteen laitenumero.

6. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tunnistuksen aikana käytetään PPP/CHAP-protokollaa RADIUS-protokollan kanssa, ja että päätelaite lähettää tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka sisältönä on käyttäjätunnus järjestelmään sekä kentän, jonka sisältönä on salasana, joka on generoitu laitetunnuksesta (IMEI), käyttäjän tilaajakohtaisesta tunnisteesta, käyttäjän henkilökohtaisesta tunnusluvusta (PIN), ajasta ja SRES-arvosta.

7. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tunnistuksen aikana käytetään PPP/PAP-protokollaa RADIUS-protokollan kanssa, ja että päätelaite lähettää tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on salasana, joka on generoitu laitetunnuksesta (IMEI), käyttäjän tilaajakohtaisesta tunnisteesta, käyttäjän henkilökohtaisesta tunnusluvusta, ajasta, ja SRES-arvosta, sekä kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka sisältönä on käyttäjätunnus järjestelmään.

8. Jonkin edellisen patenttivaatimuksen 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että salaukseen tarvittavia tietoja on tallennettu päätelaitteessa useampaan kuin yhteen tilaajakohtaiseen tunnistusmoduuliin.

9. Patenttivaatimuksen 6 tai 7 mukainen menetelmä, t u n n e t t u siitä, että käyttäjätunnus järjestelmään on käyttäjän MSISDN.

10. Järjestely käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä (102), joka järjestely käsittää

matkaviestimen (100), jota käytetään yhteyslaitteena tietokonejärjestelmään, joka matkaviestin käsittää

tilaajakohtaisen tunnistusmoduulin (342), joka sisältää tilaajakohtaisen tunnisteen,

viestimeen (100) pysyvästi koodatun laitekohtaisen tunnisteen (IMEI),

välineet (316) lukea käyttäjän syöttämä henkilökohtainen tunnusluku, joka mahdollistaa laitteen käytön,

välineet (316) tarkistaa tunnusluvun oikeellisuus ennen laitteen kutakin käyttöönottoa,

ja joka järjestely käsittää tunnistuspalvelimen (144), joka käsittää

muistivälineet tallentaa järjestelmän käyttäjien käyttäjätunnukset ja niitä vastaavat henkilökohtaiset tunnisteet ja laitekohtaiset tunnisteet,

t u n n e t t u siitä, että

matkaviestin (100) käsittää

välineet (136) generoida ensimmäinen kertakäyttöinen salasana ilman käyttäjän toimenpiteitä ennalta tunnetun algoritmin avulla käyttäjän henkilökohtaisen tunnusluvun, matkaviestimen tilaajakohtaiselta tunnistusmoduulilta (342) luetun tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen (IMEI) ja kellonajan perusteella,

välineet (136) suorittaa ensimmäisen kertakäyttöisen salasanan ja käyttäjän tilaajakohtaisen tunnisteen koodaus,

välineet (136, 338,340,300) lähettää koodatut salasana ja tilaajakohtainen tunniste tietokonejärjestelmän tunnistuspalvelimelle,

ja että tunnistuspalvelin (144) on sovitettu

suorittamaan käyttäjän tunnistus tilaajakohtaisen tunnisteen perusteella ja etsimään tietokannasta käyttäjän henkilökohtainen tunnusluku ja käyttäjään liitetyn matkaviestimen laitekohtainen tunniste (IMEI),

muodostamaan toinen kertakäyttöinen salasana tunnistuspalvelimella käyttäen ennalta määrättyä algoritmia käyttäjän henkilökohtaisen tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella,

vertaamaan ensimmäistä salasanaa ja toista salasanaa keskenään tunnistuspalvelimella, ja mikäli salasanat vastaavat, mahdollistamaan tietoliikenneyhteys käyttäjän matkaviestimen (100) ja tietokonejärjestelmän (102) välillä.

11. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) on sovitettu tahdistamaan matkaviestimen ajastus tunnistuspalvelimen (144) ajastuksen kanssa ennen tunnistusproseduurin käynnistystä.

12. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) on sovitettu suorittamaan käyttäjän tunnistus automaattisesti käyttäjän käynnistäessä tietokonejärjestelmää (102) hyödyntävän sovelluksen matkaviestimessä.

13. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että mikäli ensimmäinen ja toinen salasana eivät vastaa, tunnistuspalvelin

(144) on sovitettu olemaan lähettämättä mitään informaatiota matkaviestimelle (100).

14. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) on sovitettu lähettämään tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka sisältönä on aika, sekä kentän, jonka sisältönä on päätteen kansainvälinen puhelinnumero, sekä kentän, jonka sisältönä on päätteen laitenumero.

15. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) ja tunnistuspalvelin (144) on sovitettu tunnistuksen aikana käyttämään PPP/CHAP-protokollaa RADIUS-protokollan kanssa, ja että päätelaite on sovitettu lähettämään tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka sisältönä on käyttäjätunnus järjestelmään sekä kentän, jonka sisältönä on salasana, joka on generoitu laitetunnuksesta (IMEI), käyttäjän tilaajakohtaisesta tunnisteesta, käyttäjän henkilökohtaisesta tunnusluvusta, ajasta, SRES-arvosta.

16. Patenttivaatimuksen 10 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) ja tunnistuspalvelin (144) on sovitettu tunnistuksen aikana käyttämään PPP/PAP-protokollaa RADIUS-protokollan kanssa, ja että matkaviestin (100) on sovitettu lähettämään tunnistuspalvelimelle viestin, joka käsittää ainakin kentän, jonka sisältönä on salasana, joka on generoitu laitetunnuksesta (IMEI), käyttäjän tilaajakohtaisesta tunnisteesta, käyttäjän henkilökohtaisesta tunnusluvusta, ajasta, ja SRES-arvosta, sekä kentän, jonka sisältönä on SRES-arvo, sekä kentän, jonka sisältönä on käyttäjätunnus järjestelmään.

17. Patenttivaatimuksen 15 tai 16 mukainen järjestely, t u n n e t t u siitä, että käyttäjätunnus järjestelmään on käyttäjän MSISDN.

18. Jonkin edellisen patenttivaatimuksen 10 - 17 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) on GPRS-järjestelmän matkaviestin.

19. Jonkin edellisen patenttivaatimuksen 10 - 17 mukainen järjestely, t u n n e t t u siitä, että matkaviestin (100) käsittää useamman kuin yhden tilaajakohtaisen tunnistusmoduulin (342), ja että salaukseen tarvittavia tietoja on tallennettu useampaan kuin yhteen tunnistusmoduuliin.

(57) Tiivistelmä

Keksinnön kohteena on järjestely ja menetelmä käyttäjän luotettavaksi tunnistamiseksi tietokonejärjestelmässä (102). Menetelmässä käytetään yhteyslaitteena järjestelmään matkaviestintä (100). Menetelmässä generoidaan ensimmäinen kertakäyttöinen salasana matkaviestimessä ennalta tunnetun algoritmin avulla käyttäjän tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen (IMEI) ja kellonajan perusteella. Saatu salasana ja käyttäjän tilaajakohtainen tunniste koodataan ja lähetetään tietokonejärjestelmän (102) tunnistuspalvelimelle (144), jossa suoritetaan käyttäjän tunnistus tilaajakohtaisen tunnisteen perusteella, etsitään tietokannasta käyttäjän henkilökohtainen tunnusluku ja käyttäjään liitetyn matkaviestimen laitekohtainen tunniste, muodostetaan toinen salasana tunnistuspalvelimella käyttäen samaa määrättyä algoritmia käyttäjän henkilökohtaisen tunnusluvun, tilaajakohtaisen tunnisteen, matkaviestimen laitekohtaisen tunnisteen ja kellonajan perusteella, verrataan ensimmäistä ja toista salasanaa keskenään tunnistuspalvelimella, ja mikäli salasanat vastaavat, mahdollistetaan tietoliikenneyhteys matkaviestimen (100) ja tietokonejärjestelmän (102) välillä.

(Kuvio 1)

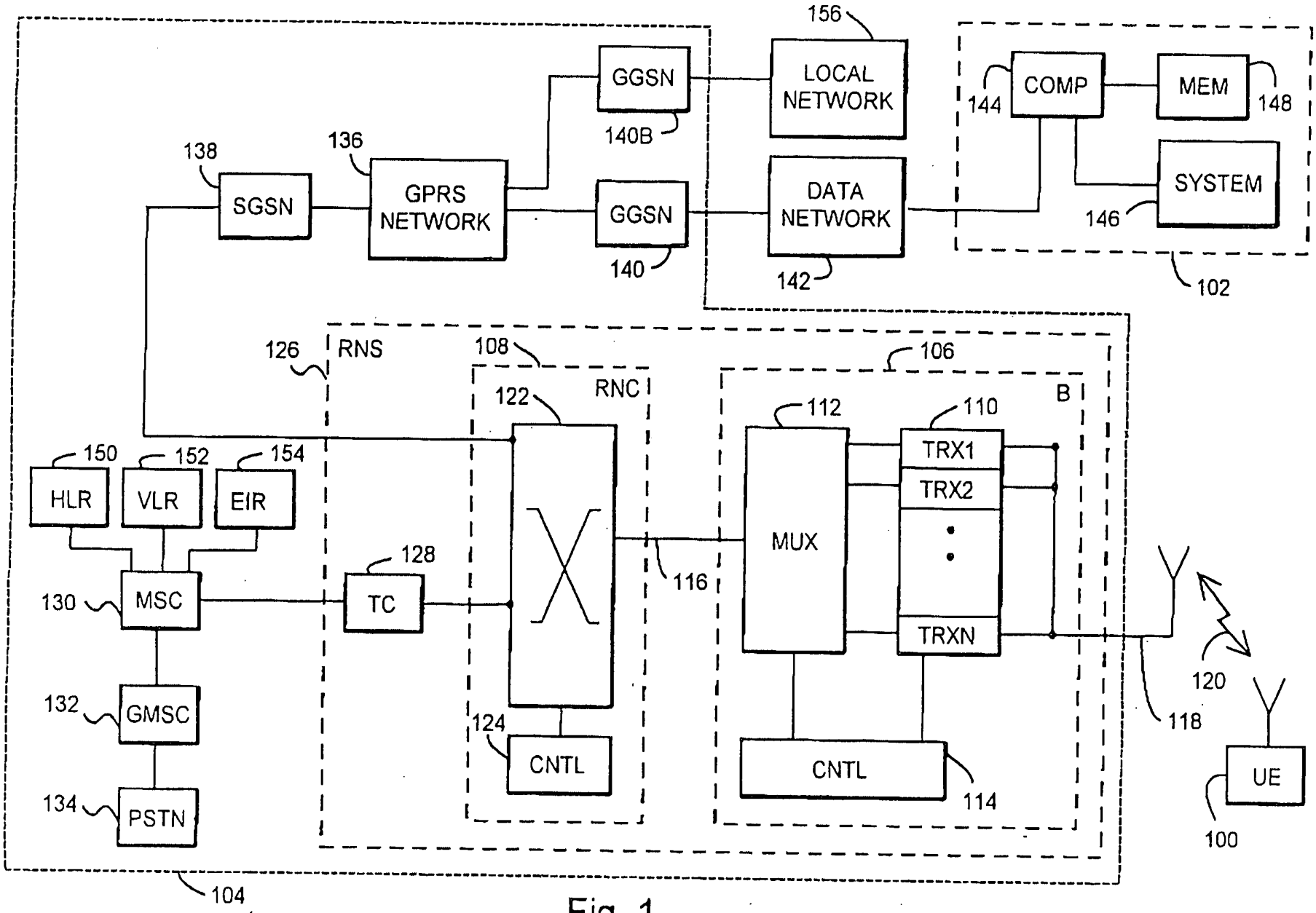
156
LOCAL NETWORK
GGSN
140B
144
COMP
MEM
148
SYSTEM
146
102
138
SGSN
136
GPRS NETWORK
GGSN
140
DATA NETWORK
142
126
RNS
108
RNC
106
B
122
112
110
TRX1
TRX2
TRXN
MUX
150
HLR
152
VLR
154
EIR
128
TC
130
MSC
116
132
GMSC
134
PSTN
124
CNTL
CNTL
114
120
118
UE
100
104

Fig. 1

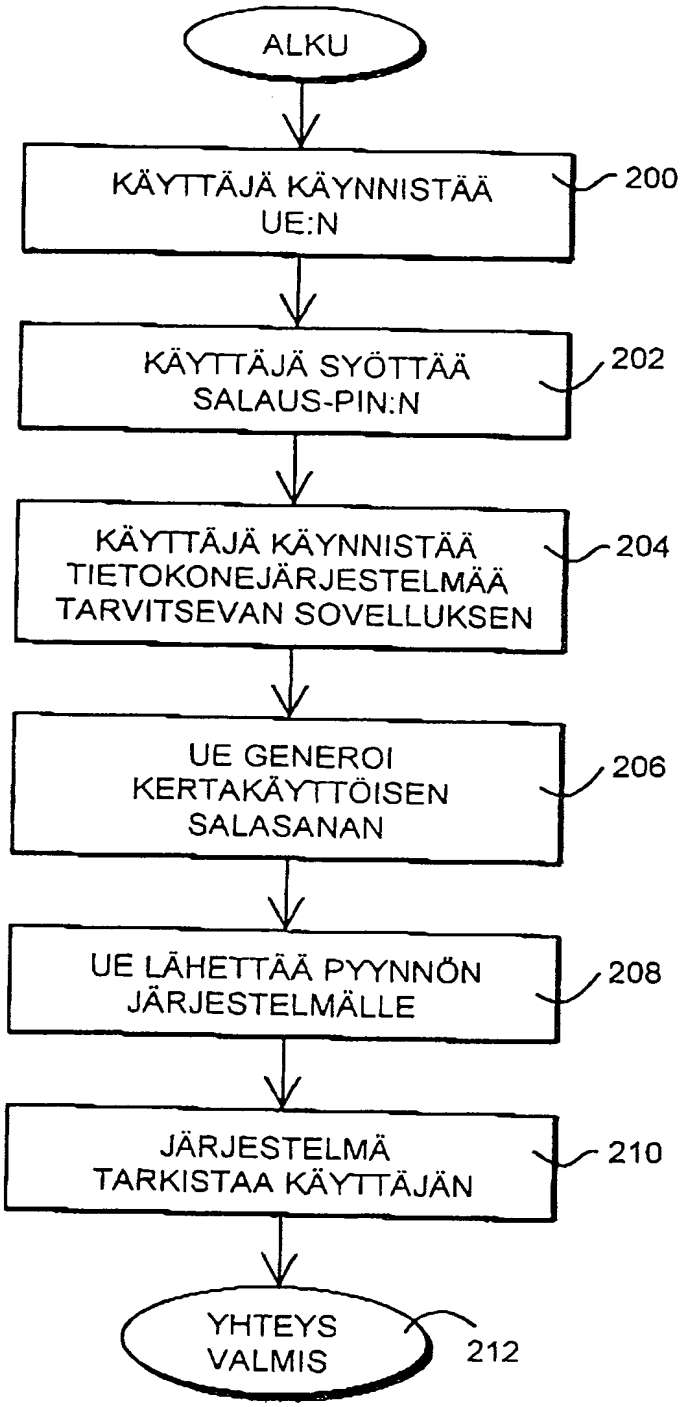
ALKU
KÄYTTÄJÄ KÄYNNISTÄÄ UE:N
200
KÄYTTÄJÄ SYÖTTÄÄ SALAUS-PIN:N
202
KÄYTTÄJÄ KÄYNNISTÄÄ TIETOKONEJÄRJESTELMÄÄ TARVITSEVAN SOVELLUKSEN
204
UE GENEROI KERTAKÄYTTÖISEN SALASANAN
206
UE LÄHETTÄÄ PYYNNÖN JÄRJESTELMÄLLE
208
JÄRJESTELMÄ TARKISTAA KÄYTTÄJÄN
210
YHTEYS VALMIS
212

Fig. 2a

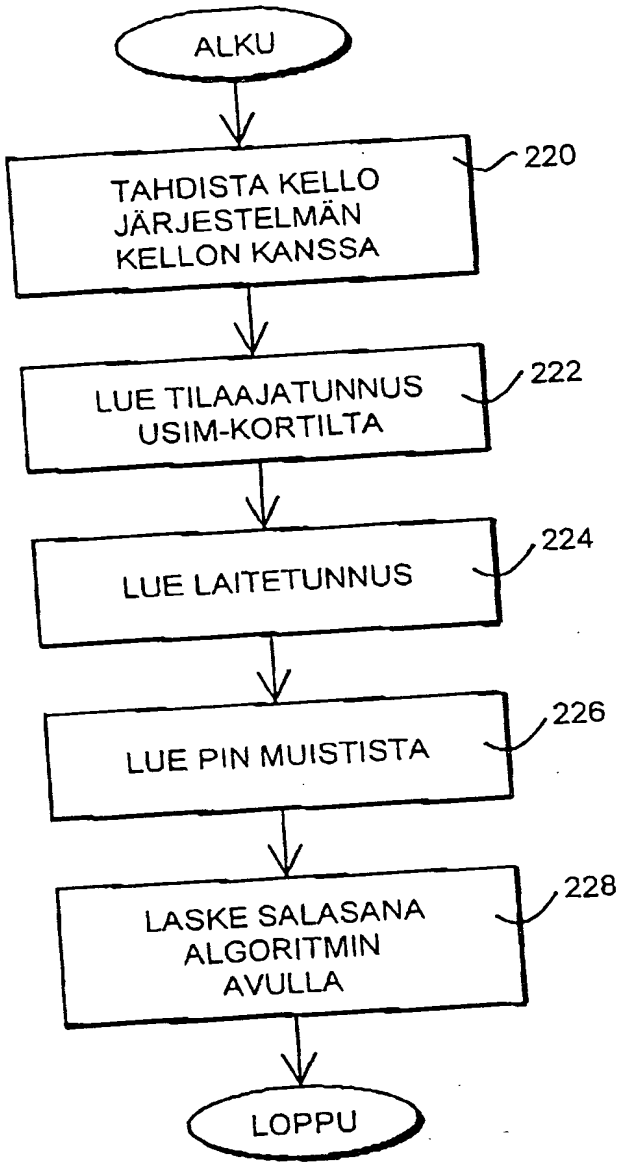
ALKU
TAHDISTA KELLO JÄRJESTELMÄN KELLON KANSSA
220
LUE TILAAJATUNNUS USIM-KORTILTA
222
LUE LAITETUNNUS
224
LUE PIN MUISTISTA
226
LASKE SALASANA ALGORITMIN AVULLA
228
LOPPU

Fig. 2b

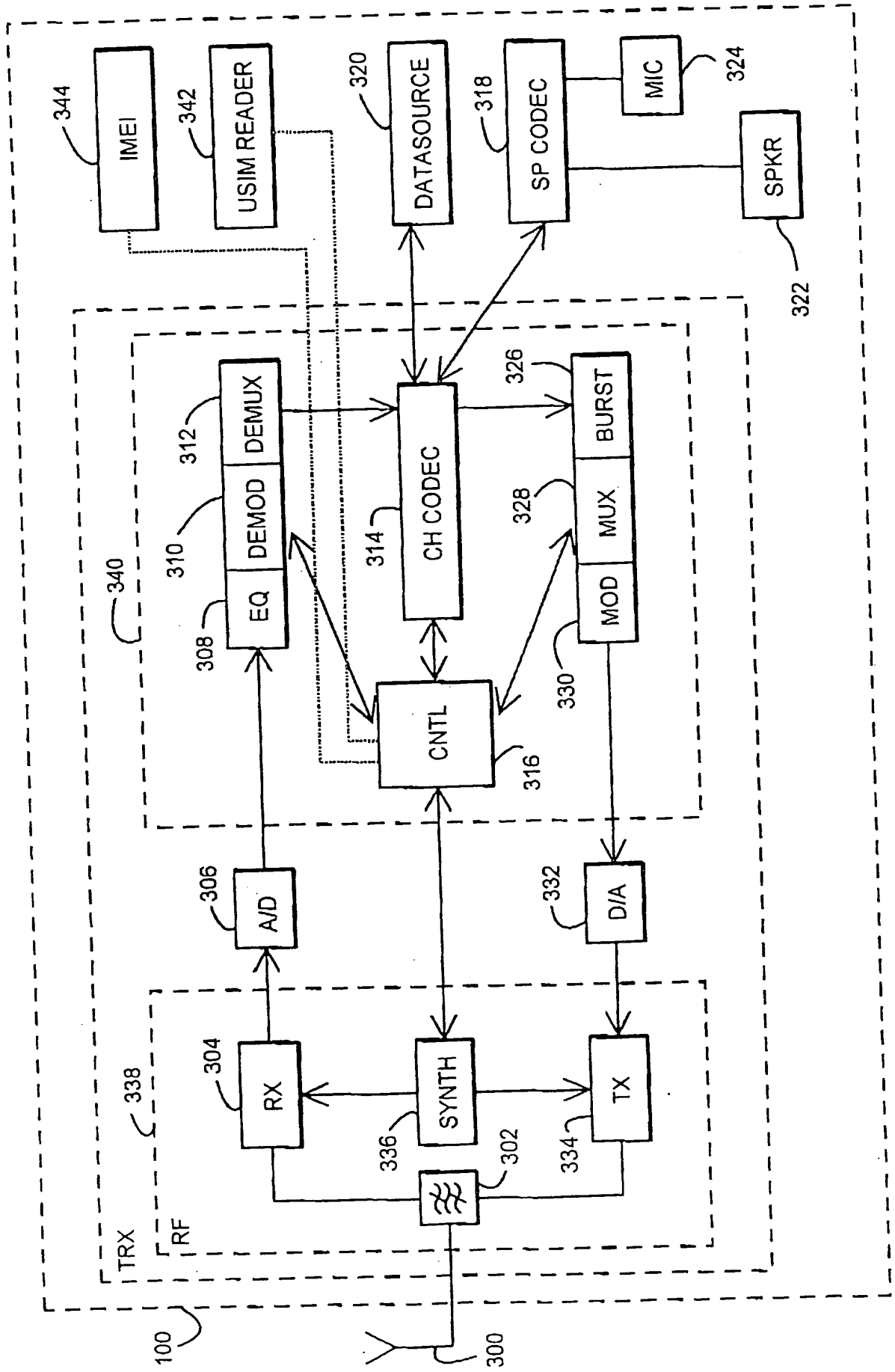
100
TRX
RF
338
RX
304
SYNTH
336
TX
334
302
300
A/D
306
D/A
332
CNTL
316
340
EQ
308
DEMOD
310
DEMUX
312
CH CODEC
314
MOD
330
MUX
328
BURST
326
IMEI
344
USIM READER
342
DATASOURCE
320
SP CODEC
318
MIC
324
SPKR
322

Fig. 3